

# The Fifth Amendment, Cell Phones and Search Incident: A Response to *Password Protected?*

Susan W. Brenner\*

I. INTRODUCTION.....	78
II. DATA SECURITY: PASSWORDS AND BEYOND.....	78
A. EVOLVING TECHNOLOGY .....	79
B. CHANGING CONCEPTIONS OF “OPEN CONTAINERS” .....	82
III. PASSWORDS, MIRANDA AND THE FIFTH AMENDMENT .....	83
A. MIRANDA .....	83
B. FIFTH AMENDMENT .....	86
IV. CONCLUSION .....	90

## I. INTRODUCTION

While I agree with much of what Professor Adam Gershowitz says in his Article *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, I believe two areas require a response. Section I of this Essay will address the first issue, the utility of password-protecting or otherwise securing the contents of cell phones. Section II of this Essay will address the second issue, the role, if any, the Fifth Amendment privilege against self-incrimination plays with regard to police requests for someone’s password.

## II. DATA SECURITY: PASSWORDS AND BEYOND

In Part III of his article, Professor Gershowitz considers whether there is any constitutional impediment to police attempting to break into a password-protected cell phone.<sup>1</sup> He finds there is not, though he notes

---

\* NCR Distinguished Professor of Law & Technology, University of Dayton School of Law.

1. See Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?*, 96 IOWA L. REV. 1125, 1147–65 (2011).

police may have a limited period of time in which to engage in such an effort.<sup>2</sup> I agree that opening locked containers is a default element of the search-incident-to-arrest exception,<sup>3</sup> and I also agree that to fall within the exception the opening of the container must not be too remote in time from the arrest that provides the justification for the entry.<sup>4</sup>

#### A. EVOLVING TECHNOLOGY

My disagreement with Part III of Professor Gershowitz's Article lies not in his analysis of the search-incident exception's applicability to cell phones, as such, but in his conclusion that "[a]t bottom, the fact that a phone is password protected does not . . . practically prevent it from being searched."<sup>5</sup> He essentially bases this conclusion on two premises. One is that given the current state of password protection for cell phones, it is not—or at least should not be—particularly difficult as a practical matter for law-enforcement officers to crack a phone's password protection.<sup>6</sup> The other is that if officers find it difficult or even impossible to crack a phone's password, they "may be able to bypass the password altogether by hacking into the phone."<sup>7</sup>

For the purposes of this Essay's analysis I am willing to accept the validity of both premises. My point of disagreement lies not so much in what Professor Gershowitz says about the possibility of breaking a password or bypassing it entirely, but in his implicit assumption that the status quo in cell-phone technology will continue for the foreseeable future. I do not believe that assumption is true.

As I've noted elsewhere, for years there has essentially been an arms race between those who are charged with defending computer systems and creating new security measures and those who quickly compromise such security (i.e., cybercriminals).<sup>8</sup> This well-established dynamic involves criminals subverting computer security measures that are intended to protect vulnerable, legitimate targets from their unlawful efforts.

This dynamic is not the only manifestation of the arms race between the "good guys" and cybercriminals.<sup>9</sup> For years, evidence has shown that

---

2. See *id.* at 1161–65.

3. See, e.g., *United States v. Vinton*, 594 F.3d 14, 25–26 (D.C. Cir. 2010) (upholding the forced opening of a locked briefcase found in the arrestee's vehicle as a proper search incident under *Arizona v. Gant*, 129 S.Ct. 1710 (2000)), *cert. denied*, 113 S. Ct. 93 (2010).

4. See Gershowitz, *supra* note 1, at 1161–65.

5. *Id.* at 1165.

6. See *id.* at 1164–65.

7. *Id.* at 1164.

8. See, e.g., Susan W. Brenner, "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare, 97 J. CRIM. L. & CRIMINOLOGY 379, 449 n.319 (2007).

9. For the purposes of this analysis, I define "cybercriminal" as someone who uses computer technology to engage in unlawful acts that (1) are directed at computer systems (e.g., hacking, malware, Distributed Denial of Service attacks); or (2) use computer technology as a

cybercriminals know how to use strong encryption for their own ends, such as preventing law-enforcement officers from gaining access to incriminating data.<sup>10</sup> We do not know precisely how widespread the use of encryption is among cybercriminals, but I, for one, believe its use is more common among cybercriminals than it is among traditional “street” criminals.<sup>11</sup>

It is reasonable to infer that cybercriminals are more likely to use encryption than their traditional colleagues, because cybercriminals tend to use technology more intensely and in more sophisticated ways than street criminals, at least for the present. Street criminals—who so far seem to be the primary, if not the exclusive, targets of cell phone searches predicated on the search-incident-to-arrest exception—tend to use computer technology in a fashion similar to that of the average citizen. That is, they use computers and cell phones without being aware of the need for, and availability of, technical measures that can protect the privacy and security of their data.

I base this inference on several factors, the most obvious of which is that street criminals really have no reason to become sophisticated users of computer technology. Cybercriminals operate in an environment that is created and sustained by computer technology and therefore understand that technology can be exploited in diverse and devious ways. Street criminals operate in the physical world, using computer technology primarily to communicate with each other, friends, family, and on occasion, actual or potential victims.<sup>12</sup> Their use of computer technology is minimal—on a par with how average law-abiding citizens use the technology.<sup>13</sup>

Average citizens, law-abiding or otherwise, tend not to realize that there are good reasons—including privacy and security—to protect their hard drives, cell phones, and other electronic devices.<sup>14</sup> Even if they realize the need to secure their systems, they may not understand how to do so.<sup>15</sup> This lack of knowledge and ability accounts for the fact that (1) it is relatively

---

tool in the commission of traditional crimes (e.g., online fraud, stalking, harassment, theft). *See, e.g.*, SUSAN W. BRENNER, *CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE* 39–44 (2010).

10. *See, e.g.*, KEVIN POULSEN, *KINGPIN: HOW ONE HACKER TOOK OVER THE BILLION-DOLLAR CYBERCRIME UNDERGROUND* 198–200 (2011).

11. For the purposes of this analysis, I define “street” criminals as those who commit traditional crimes in essentially traditional ways (e.g., drug dealers, pimps, members of gangs that commit crimes such as assault, murder, and theft). While they use cell phones and other technology, their use of technology plays such a minor role in the commission of their offenses that they do not qualify as cybercriminals. *See, e.g.*, BRENNER, *supra* note 9, at 45–47.

12. *See, e.g.*, *United States v. Arellano*, No. 09-5012, 2011 WL 397736, at \*2 (4th Cir. Feb. 8, 2011); *People v. Diaz*, 244 P.3d 501, 502–03 (Cal. 2011); *Hawkins v. State*, 704 S.E.2d 886, 888 (Ga. Ct. App. 2010).

13. *See supra* note 12 and accompanying text.

14. *See, e.g.*, Ben Worthen, *Most People Don't Understand Cyber Threats, Says Former DHS Chief*, WALL ST. J. (Mar. 3, 2010), <http://blogs.wsj.com/digits/2010/03/03/most-people-don%E2%80%99t-understand-cyber-threats-says-former-dhs-chief/>.

15. *See id.*

unusual for street criminals to take steps to secure their cell phones or computers, and (2) when they make such an effort, they tend to use password-protection, at most.<sup>16</sup>

There are only a few cases involving defendants who took the additional step of encrypting their hard drives,<sup>17</sup> and they involve cybercriminals rather than street criminals. It seems there are no reported cases, or anecdotal evidence, involving street criminals who made an effort to encrypt their cell phones (or computers).

While few, if any, average citizens currently protect their technology, I suspect this state of affairs will change; street criminals as well as their law-abiding counterparts will begin to use technology that is currently available to, or at least used by, only the tech-savvy. Indeed, anecdotal evidence indicates a demand for stronger encryption is emerging, prompted by a “surge” of attacks on cell phones and other mobile devices.<sup>18</sup> At the same time, technology commentators are questioning the robustness of existing technology to protect private electronic data. Noting Professor Gershowitz’s point that it is relatively easy for law-enforcement officers to crack cell-phone passwords or bypass them entirely by hacking the phone,<sup>19</sup> these commentators point out that the better approach is “full-disk encryption” of cell phones: “While it isn’t absolutely foolproof, full-disk encryption is the most reliable and practical method for safeguarding your smartphone data from the prying eyes of law enforcement officers.”<sup>20</sup> Until recently, however, full-disk encryption for cell phones was not widely available, but cell-phone companies have started to add encryption features, which vary in robustness.<sup>21</sup>

Another factor that may result in the widespread availability of robust cell-phone encryption is recent efforts by the United States military to utilize such technology. In April of 2011, the Defense Advanced Research Projects Agency (“DARPA”) announced that it was seeking “new technologies and methods to support full disk and system encryption of the commercial mobile devices—specifically Apple and Android platforms—to include a pre-

---

16. See, e.g., *United States v. Mohr*, No. 10-13154, 2011 WL 1057546, at \*1 (11th Cir. Mar. 24, 2011) (computer); *People v. Villasana*, No. Fo56773, 2010 WL 7122, at \*1 (Cal. Ct. App. Jan. 4, 2010) (cell phone), *cert. denied*, 131 S. Ct. 212 (2010).

17. See, e.g., *United States v. Aleyikov*, No. 10 Cr 96(DLC), 2011 WL 939754, at \*4 (S.D.N.Y. Mar. 16, 2011) (involving a defendant who encrypted data taken from his employer before uploading it to an offshore “subversion” website and then deleted the encryption key).

18. See, e.g., Ryan Radia, *Why You Should Always Encrypt Your Smartphone*, ARS TECHNICA (Jan. 16, 2011), <http://arstechnica.com/gadgets/guides/2011/01/why-you-should-always-encrypt-your-smartphone.ars/>.

19. See, e.g., *id.*

20. *Id.*

21. See *id.* (explaining that more robust encryption is available on the BlackBerry while less robust encryption is available for the iPhone and Windows Phone 7).

boot environment to load the operating system.”<sup>22</sup> DARPA is asking “industry and universities to submit . . . ideas/concepts that . . . can be deployed in less than 90 days.”<sup>23</sup> While the DARPA solicitation is concerned only with improving the security of military cell phones, it may also spur advances in civilian cell-phone encryption as well, both because of the emphasis the military is placing on cell-phone privacy and because DARPA projects often influence civilian technology.<sup>24</sup>

Thus, society cannot assume to continuance and eventual permanency of the current state of affairs of cell-phone security. Instead, an increased use of encryption and other data-protection measures will make it increasingly difficult, if not impossible, for officers to access a cell phone’s contents.

### B. CHANGING CONCEPTIONS OF “OPEN CONTAINERS”

That, however, is only one way in which things are likely to change. The electronic devices used today (e.g., computers, cell phones) are functionally analogous to the tangible containers traditionally involved in searches incident to arrest. Electronic devices store intangible data instead of tangible items, like drugs, weapons, etc., but they are free-standing “containers.” When an officer arrests someone who is carrying a cell phone (or, arguably, a laptop), conducts a search incident to arrest, and seizes the cell phone (or laptop), the officer has engaged in the traditional, search-incident dynamic. That is, he has effected a zero-sum seizure of a “container” from the person under arrest and, under the search-incident exception, is entitled to “open” the container and examine its contents. Of course, unlike a traditional container, the contents of which are stored within its physical parameters, cell phones (and laptops) have the added capacity to access additional content that is stored elsewhere. Seemingly, courts have not addressed the propriety of an officer using a cell phone (or laptop) to access offsite data under the authority of the search-incident-to-arrest exception.<sup>25</sup>

Remote server networks and off-site data storage may become the critical issue in search-incident-to-arrest law.<sup>26</sup> One of the factors that may

---

22. Michael Cooney, *Military Wants Full Disk Encryption for iPhone, Android Smartphones*, NETWORKWORLD (Apr. 12, 2011), <http://www.networkworld.com/community/blog/military-wants-full-disk-encryption-iphone-an> (quoting *Request for Information (RFI) for Full Disk Encryption Method for Commercial Mobile Devices*, FEDBIZOPPS.GOV (Apr. 11, 2011) <https://www.fbo.gov/index?s=opportunity&mode=form&id=3473e17cb0615b10d9c93533180aa345&tab=core&tabmode=list&>) (internal quotation marks omitted).

23. *Id.*

24. *See id.*

25. *See generally* Chandler v. State, No. 49A02-0903-CR-264, 2010 WL 183437, at \*8 n.5 (Ind. Ct. App. Mar. 25, 2010) (declining to find a search and seizure when an officer called his own cell phone from an arrestee’s cell phone to obtain the arrestee’s cell phone number).

26. Indeed, many believe that “by 2020 most people will access software applications online and share and access information through the use of remote server networks, rather than depending . . . on tools and information housed on their individual” cell phones and computers. JANA QUITNEY ANDERSON & LEE RAINIE, PEW INTERNET & AM. LIFE PROJECT, THE

drive this development is a concern with security; cybercriminals are increasingly targeting cell phones and other mobile devices. Many see the use of cloud computing as the best way to address this rising threat.<sup>27</sup> So, instead of accessing data stored on an individual cell phone, a cybercriminal or a law enforcement officer conducting a search incident to arrest will have to access data that is stored on an off-site system with advanced security measures. Because these off-site storage networks are likely to include encryption,<sup>28</sup> it is unlikely that law enforcement will be able to break the security available on sites like these.

The goal for this Section is essentially to reiterate what Justice Brandeis said in his *Olmstead* dissent: “[i]n the application of a Constitution, . . . our contemplation cannot be only of what has been but of what may be.”<sup>29</sup> Brandeis was arguing for a flexible interpretation of the Fourth Amendment, one that could encompass the then-novel issues generated by citizens’ use of the telephone.<sup>30</sup> In this Section, I argue for something similar, but more modest: the proposition that the current state of cell phone technology is limited when compared to its future. Given that, society should not dismiss the Fifth Amendment’s effect on the application of the search-incident exception to cell phones and more evolved mobile devices.

### III. PASSWORDS, MIRANDA AND THE FIFTH AMENDMENT

In this Part, I examine the applicability of the Fifth Amendment privilege against self-incrimination and/or the “prophylactic rules” the Supreme Court created in *Miranda v. Arizona*<sup>31</sup> to the elicitation of the password needed to access the contents of a secured cell phone. The first Subpart below examines the extent to which *Miranda* applies in this context; the next Subpart examines the Fifth Amendment’s applicability to this issue.

#### A. MIRANDA

In *Miranda*, the Court held that “the prosecution may not use statements . . . stemming from custodial interrogation of the defendant unless it demonstrates the use of procedural safeguards effective to secure the privilege against self-incrimination.”<sup>32</sup> It defined “custodial interrogation” as “questioning initiated by law enforcement officers after a

---

FUTURE OF CLOUD COMPUTING 2 (2010), available at [http://pewresearch.org/~media/Files/Reports/2010/PIP\\_Future\\_of\\_the\\_Internet\\_cloud\\_computing.pdf](http://pewresearch.org/~media/Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf).

27. See, e.g., Olafur Ingthorsson, *Smartphone Security and the Mobile Cloud*, DATA CTR. KNOWLEDGE (Apr. 12, 2011), <http://www.datacenterknowledge.com/archives/2011/04/12/smartphone-security-and-the-mobile-cloud/>.

28. See *id.*

29. *Olmstead v. United States*, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

30. See *id.*

31. *Miranda v. Arizona*, 384 U.S. 436 (1966); see, e.g., *Connecticut v. Barrett*, 479 U.S. 523, 528 (1987).

32. *Miranda*, 384 U.S. at 444.

person has been taken into custody or otherwise deprived of his freedom of action in any significant way.”<sup>33</sup> The “procedural safeguards” consist of warning the suspect of his right to remain silent and his right to counsel, after which it is up to the suspect to invoke or waive either or both rights.<sup>34</sup>

We will use a simple scenario to analyze the potential *Miranda* issues that can arise from a custodial arrest followed by a search incident involving a cell phone: assume Officer Doe arrests John Roe for operating a stolen vehicle. Doe clearly has probable cause to make the arrest, and since he has arrested Roe, the search-incident exception applies to authorize a search of Roe’s person, which includes whatever he has in his pockets. As Doe searches Roe, he finds a cell phone in Roe’s pocket, seizes it, and opens the phone to look through its contents. The phone, though, is encrypted and, therefore, locked.

When he realizes the cell phone is locked, Doe turns to Roe and says, “Your phone’s encrypted. I need to search it; give me the password.” Since Roe has been arrested, he is in “custody” for *Miranda* purposes,<sup>35</sup> which means the prosecution cannot use any “statements” he makes unless and until he is given the *Miranda* warning and waives his rights to silence and counsel. Doe’s telling Roe to give him the password constitutes “interrogation” for *Miranda* purposes,<sup>36</sup> but Doe did not *Mirandize* Roe before initiating the interrogation.

Doe has, therefore, violated *Miranda*, which means the prosecution will not be able to use any “statement” Roe makes in response to Doe’s question. Since we are assuming Roe’s cell phone is encrypted, there are four potential ways in which he can respond to Doe’s interrogation: (1) refuse to respond (and, perhaps, ask for a lawyer); (2) orally provide the password; (3) physically provide the password; and (4) electronically provide the password.

The first response obviously eliminates the need to consider the admissibility of any responses to Doe’s interrogation. The second response almost certainly constitutes a “statement” that would have to be suppressed under *Miranda*. The Supreme Court does not appear to have defined the term *statement* as it is used in this context, but a dictionary defines it as “a definite or clear expression of something in speech or writing.”<sup>37</sup> The statement itself therefore would be suppressed, but the physical fruits of the

---

33. *Id.*

34. *Id.* at 444–45.

35. *See, e.g.,* Murray v. Earle, 405 F.3d 278, 286 (5th Cir. 2005).

36. *See* Rhode Island v. Innis, 446 U.S. 291, 300–01 (1980) (elucidating that *Miranda* interrogation encompasses “express questioning *or* its functional equivalent”, and includes “any words or actions on the part of the police . . . [they] should know are reasonably likely to elicit an incriminating response.”).

37. CONCISE OXFORD ENGLISH DICTIONARY 1402 (J. Pearsall ed., rev. 10th ed. 2001).

violation, which would presumably extend to the contents of the cell phone, probably would not.<sup>38</sup>

In the third response, the encrypted phone is accessed with a biometric key, as where Roe puts his right index finger on a biometric reader. The reader identifies Roe and unlocks the phone, giving Doe access to data it contains. If Roe's placing his finger on the biometric reader constitutes a statement within the compass of *Miranda*, then the statement itself would have to be suppressed under *Miranda*. Roe's lawyer could argue that Roe's placing his finger on the biometric reader constitutes a statement under either of two theories: the first is that it is a nonverbal communication, e.g., the equivalent of nodding, and, as such, qualifies as a statement under *Miranda*. Since courts have held that nonverbal acts can constitute such a statement, Roe might succeed in suppressing the act under this theory.<sup>39</sup> Whether he could also succeed in suppressing the data retrieved from the cell phone would depend on whether a court found that the data was merely the physical fruits of the *Miranda* violation.

The other theory is that Roe's act of placing his finger on the biometric reader constitutes "testimony" under *Fisher v. United States*.<sup>40</sup> In *Fisher*, the Court held that the act of producing evidence is "testimony" within the scope of the Fifth Amendment privilege if the act concedes that (1) the evidence exists; (2) the evidence is within the person's possession and control; and (3) the evidence is authenticated, i.e., the person believes that it is the evidence sought.<sup>41</sup> For the purposes of this analysis, assume that the "testimony" within the scope of the Fifth Amendment privilege is equivalent to "statements" with the compass of the *Miranda* rules.<sup>42</sup> Roe's lawyer could argue that Roe's placing his finger on the biometric reader constituted testimony under this standard because it implicitly conceded that (1) the "password" Doe asked for existed; (2) was within Roe's possession and control; and (3) indicated Roe's belief that placing his finger on the reader would provide the password that Doe sought.

The act of producing evidence will not be testimonial under *Fisher* if the "existence and location" of the evidence is "a foregone conclusion," so the act "adds little or nothing" to the government's information.<sup>43</sup> Here, the prosecution could argue that it was a foregone conclusion that a password

38. See *United States v. Patane*, 542 U.S. 630, 637-638 (2004) (stating that "nontestimonial evidence" need not be suppressed).

39. See, e.g., *United States v. Dillard*, No. 2:09-cr-00057-RLH-GWF, 2010 WL 5764682, at \*11 (D.C. Nev. Dec. 16, 2010) ("[D]efendant's . . . verbal and non-verbal statements . . . should be suppressed because he was in custody and was not advised of his *Miranda* rights.")

40. *Fisher v. United States*, 425 U.S. 391 (1976).

41. See *id.* at 410-11.

42. I believe this is a reasonable assumption, given that *Miranda* is designed to protect the privilege against self-incrimination. See *supra* note 32 and accompanying text; see also *Miranda v. Arizona*, 384 U.S. 436, 457-58 (1966).

43. *Fisher*, 425 U.S. at 411.

existed for the phone and that Roe had it.<sup>44</sup> Roe's lawyer could argue that while it might be a foregone conclusion that an encrypted phone had a password, it was not a foregone conclusion that Roe had it. If a court found that Roe's act of placing his finger on the biometric reader was a testimonial act, then evidence of that act would have to be suppressed. Whether he could also succeed in suppressing the data retrieved from the cell phone would depend on whether a court found that the data was merely the physical fruits of the *Miranda* violation.

The *Miranda* analysis of the fourth response, in which Roe uses a token to unlock the phone, is very similar to the analysis of the third response, but it differs in at least one respect from the analysis of the preceding scenario: in that scenario, Roe personally unlocks the phone by putting his finger on the reader; in this scenario, he uses a token to do so. Here, the prosecution may argue that Roe's conduct is the equivalent neither of nonverbal communication nor a testimonial act of producing evidence under *Fisher*. In his dissent in *Doe v. United States*, Justice Stevens noted that an arrestee "may . . . be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed."<sup>45</sup> I can see the prosecution arguing that while Roe's placing his finger on the biometric reader could constitute testimony under this observation (since he would, in effect, be revealing the combination to a locked container), his using a token to unlock the phone is the functional equivalent of producing the key to a strongbox and therefore does not constitute testimony or a statement under *Miranda*.

#### B. FIFTH AMENDMENT

This Subpart analyzes two different scenarios of the Roe–Doe fact pattern in which the Fifth Amendment privilege against self-incrimination might apply. The first scenario arises when Roe refuses to provide the password (via any means) and asks for a lawyer, which would presumably trigger the *Miranda* right to counsel and preclude Doe from making further inquiries about the password.<sup>46</sup> The scenario continues with a prosecutor having a grand jury issue a subpoena that orders Roe to appear and testify, his testimony to include providing the password to his cell phone.<sup>47</sup>

---

44. See, e.g., *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718, at \*3 (D.C. Vt. Feb. 19, 2009).

45. *Doe v. United States*, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting).

46. See *Edwards v. Arizona*, 451 U.S. 477, 484–85 (1981). This result could also arise if we modified the scenario so Doe administered *Miranda* warnings to Roe; Roe invoked his right to counsel; and Doe ceased his efforts to obtain the password.

47. For a similar scenario, see *In re Boucher*, 2007 WL 4246473, at \*1–2. Subpoenaing Roe to testify before a grand jury would presumably not violate his invocation of the *Miranda* right to counsel because the *Miranda* rules do not apply to grand jury proceedings. See *United States v. Mandujano*, 425 U.S. 564, 579–80 (1976).

Roe moves to quash the subpoena, claiming it violates his privilege against self-incrimination; his claim is predicated on the premise that orally providing the password constitutes “testimony” that violates the Fifth Amendment.<sup>48</sup> To successfully claim the privilege, Roe must show that he is being compelled to give testimony that is incriminating.<sup>49</sup> The subpoena establishes compulsion, since a witness must comply or be held in contempt.<sup>50</sup> Roe’s reciting the password constitutes “testimony” under the Fifth Amendment, and we are assuming the password will lead the government to incriminating evidence.<sup>51</sup> Clearly then, Roe could claim the privilege and refuse to provide the password.<sup>52</sup> The prosecution could override Roe’s invoking the privilege and compel him to provide the password if it provided him immunity for the act of producing the evidence at issue; the immunity would encompass any derivative use of evidence produced pursuant to the grant of immunity.<sup>53</sup>

The second scenario is the one Professor Gershowitz describes as the “police demand[ing] . . . that an arrestee provide his password and the arrestee compl[ing] out of a belief that he has no choice.”<sup>54</sup> Professor Gershowitz analyzes whether in this scenario police have violated the arrestee’s Fifth Amendment privilege against self-incrimination (as opposed to *Miranda*) and ultimately concludes they have not.<sup>55</sup> As discussed above, and as Professor Gershowitz notes, to claim the privilege, one must be compelled to give testimony that is incriminating.<sup>56</sup> Professor Gershowitz ultimately concludes that the scenario does not implicate the Fifth Amendment privilege because, while it involves eliciting “testimony” that is “incriminating”, it does not involve “compulsion.”<sup>57</sup>

48. See, e.g., *In re Boucher*, 2007 WL 4246473, at \*5–6.

49. See, e.g., SUSAN W. BRENNER & LORI E. SHAW, FEDERAL GRAND JURY: A GUIDE TO LAW AND PRACTICE § 12:3 (2006); see also Gershowitz, *supra* note 1, at 1168.

50. BRENNER & SHAW, *supra* note 49, at § 10:42.

51. See *Hoffman v. United States*, 341 U.S. 479, 486 (1951) (explaining that the privilege applies to answers that would themselves “support a conviction under a . . . criminal statute” and to “those which would furnish a link in the chain of evidence needed to prosecute the claimant” for a crime). The password itself may or may not be incriminating, but if it provides a link in the chain of evidence that could lead to a conviction, it can support a claim of the privilege.

52. See, e.g., *United States v. Kirschner*, No. 09-MC-50872, 2010 WL 1257355, at \*3 (E.D. Mich. Mar. 30, 2010) (allowing the defendant to take the privilege and refuse “to reveal the password for” certain “computer [communications]”); *In re Boucher*, 2007 WL 4246473 (allowing the defendant to claim the privilege and refuse to reveal the password for his encrypted computer).

53. See, e.g., *United States v. Hubbell*, 530 U.S. 27, 38–39 (2000).

54. Gershowitz, *supra* note 1, at 1168.

55. See *id.* at 1168–74.

56. See *id.* at 1168; see also *supra* note 49, and accompanying text.

57. See Gershowitz, *supra* note 1, at 1168–74. As we saw earlier, “testimony” within the compass of the Fifth Amendment privilege is the equivalent of, or subsumes, the “statements” encompassed by *Miranda*. See *supra* note 42 and accompanying text.

The argument that police cannot “compel” someone to testify in a fashion that violates the Fifth Amendment or, more precisely, in the fashion that violated the Fifth Amendment prior to the Supreme Court’s decision in *Miranda v. Arizona* is persuasive. As I understand the Fifth Amendment privilege, its origins lie in the English ecclesiastical courts’ use of the ex officio oath.<sup>58</sup> A witness who refused to take the oath could face certain consequences.<sup>59</sup> As the Supreme Court has noted, the privilege was intended to free witnesses from the “cruel trilemma” of remaining silent and facing various penalties, telling the truth and incriminating themselves, or committing perjury. The privilege therefore traditionally was not “applied to situations arising in the police station because the police have no legal power to compel testimony.”<sup>60</sup>

The *Miranda* Court changed that because it was “satisfied that all the principles embodied in the privilege apply to informal compulsion exerted by law-enforcement officers during in-custody questioning.”<sup>61</sup> It noted that “the Fifth Amendment privilege . . . serves to protect persons in all settings in which their freedom of action is curtailed in any significant way from being compelled to incriminate themselves.”<sup>62</sup> And in *Rhode Island v. Innis*, the Court held that the “procedural safeguards outlined in *Miranda* are not required” when “a suspect is simply taken into custody, but rather where a suspect in custody is subjected to interrogation,” because interrogation involves “a measure of compulsion above and beyond that inherent in custody.”<sup>63</sup>

The *Miranda* Court therefore held that the combination of custody and police interrogation established the compulsion required for the application of the Fifth Amendment privilege against self-incrimination.<sup>64</sup> In our original scenario,<sup>65</sup> Roe is in custody and has been subjected to interrogation by Doe. Why, then, does the Fifth Amendment privilege, as such, not apply? One argument might be that the privilege does not apply with full force, because the measure of compulsion Doe can impose is significantly less than the sanctions a court can impose on a recalcitrant

58. See, e.g., R.H. Helmholz, *Origins of the Privilege Against Self-Incrimination: The Role of the European IUS Commune*, 65 N.Y.U. L. REV. 962, 965–67 (1990).

59. See, e.g., Neill H. Alford, Jr., *The Right of Silence*, 79 YALE L.J. 1618, 1618–20 (1970) (reviewing LEONARD W. LEVY, *ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION* (1968)).

60. Note, *Tacit Criminal Admissions*, 112 U. PA. L. REV. 210, 247 (1963) (citing 8 WIGMORE, *EVIDENCE* § 2252, at 328–29 (McNaughton rev. 1961)).

61. *Miranda v. Arizona*, 384 U.S. 436, 461 (1966).

62. *Id.* at 467.

63. *Rhode Island v. Innis*, 446 U.S. 221, 300 (1980).

64. *Miranda*, 384 U.S. at 444. As Professor Gershowitz notes, this conclusion is also supported by the Court’s decision in *Bram v. United States*, 168 U.S. 532 (1897). See Gershowitz, *supra* note 1, at 1169.

65. See *supra* Part III.A.

witness. The problem I see with that argument is that in *Miranda*, the Supreme Court gave suspects who are subjected to custodial interrogation more protection than is provided by the Fifth Amendment itself, because of the particular “evils” involved in custodial interrogation.<sup>66</sup> It is, of course, possible that the *Miranda* Court meant for the procedural safeguards it established for custodial police interrogation to displace the traditional Fifth Amendment dynamic, so that if one is given *Miranda* warnings and waives the *Miranda* rights courts will conclusively presume that he or she was not “compelled” to speak.

Doe, though, did not *Mirandize* Roe before interrogating him about the cell-phone key, which apparently means the presumption hypothesized above cannot apply in this case. If the presumption does not apply, does that mean Roe was “compelled” to speak in violation of his Fifth Amendment privilege? The Supreme Court has held that a failure to administer *Miranda* warnings “creates a presumption of compulsion” that bars the prosecution from using “unwarned statement[s]” in its case in chief.<sup>67</sup>

That holding brings us to the critical issue this second scenario raises. As we saw earlier, Doe’s failure to *Mirandize* Roe means that Roe’s “statements”<sup>68</sup> concerning the cell phone password would be suppressed. Why, then, would Roe want to argue that Doe’s conduct violated his Fifth Amendment privilege against self-incrimination?

There are three ways in which Roe could benefit from establishing that Doe’s conduct violated the Fifth Amendment, as well as *Miranda*. Under *Miranda*, Doe’s conduct results in the suppression of Roe’s “statements” but not the physical fruits of those statements. If the data retrieved from Roe’s cell phone is considered physical evidence, it will not be excluded; if, on the other hand, the data is considered to be a “statement” in its own right, it should be excluded. A prosecutor could argue that we arrive at the same result under the Fifth Amendment because the Court has found that the privilege contains “its own” exclusionary rule,<sup>69</sup> which only applies to compelled “testimony.”<sup>70</sup> Roe could respond by arguing that his act of producing the evidence was incriminating testimony that was compelled by Doe and that under the Supreme Court’s decision in *United States v. Hubbell* the prosecution was barred from using evidence it obtained as a result of that testimony. This approach might give Roe a way to avoid the *Patane* principle noted earlier.

---

66. See *United States v. Mandujano*, 425 U.S. 564, 573–81 (1976) (stating that there is no right to silence or right to counsel under the Fifth Amendment); *id.* at 579–80 (exploring the unique evils of interrogation).

67. *Oregon v. Elstad*, 470 U.S. 298, 307 (1985).

68. See *supra* Part III.A.

69. *United States v. Patane*, 542 U.S. 630, 640 (2004).

70. See *id.* at 638.

Another possibility involves the use of statements to impeach a defendant who testifies at trial. Statements taken in violation of *Miranda* can be used to impeach; statements taken in violation of the Fifth Amendment privilege cannot.<sup>71</sup> So, Roe could use the argument that Doe's actions violated his Fifth Amendment privilege (as well as *Miranda*) in an effort to prevent the prosecution from using any of the "statements" he made about the password to impeach his testimony at trial.

The third possibility involves preventing the prosecution from relying on an exception to the *Miranda* rules, such as the public-safety exception. The public-safety exception allows the prosecution to use statements taken in violation of *Miranda* and statements that would otherwise be the "illegal fruits" of the *Miranda* violation if the officer acted out of a "need for answers to questions in a situation posing a threat to the public safety."<sup>72</sup> If the prosecution could show that Doe asked for the password without *Mirandizing* Roe because he was dealing with a situation that involved a threat to public safety, it could use Roe's statements in its case in chief. Therefore, if Roe were charged with a crime—terrorism, for example—he could argue that Doe's conduct violated the Fifth Amendment privilege, as well as *Miranda*, in an effort to avoid application of the public-safety exception and prevent the use of the evidence at his trial.<sup>73</sup>

#### IV. CONCLUSION

Part II hypothesizes that as familiarity with and understanding of the implications of using cell phones and other electronic devices increases, people will increasingly use encryption and other measures to protect the privacy of their data. I suspect that the often cavalier attitude many of us currently display toward that issue is at least to some extent due to ignorance of precisely how much information is stored on those devices; we are, after all, not that far removed from the era when, absent wiretaps or special recording devices, the contents of phone calls evaporated as they were generated. In that environment, there was little reason to be concerned about ensuring privacy, since there was little one could do, other than perhaps using phone booths.<sup>74</sup>

In our world, there are many reasons to be concerned about ensuring privacy. There are also an increasing number of measures we can take to implement that concern, such as password protection and encrypted data. As explained in Part II, people will increasingly take advantage of those measures by implementing technical systems that make it difficult, if not impossible, to access data stored on our personal devices.

---

71. Compare *Oregon v. Hass*, 420 U.S. 714, 722–23 (1975), with *New Jersey v. Portash*, 440 U.S. 450, 459 (1979).

72. *New York v. Quarles*, 467 U.S. 649, 657–58 (1984).

73. See, e.g., *United States v. Khalil*, 214 F.3d 111, 121 (2d Cir. 2000).

74. See, e.g., *Katz v. United States*, 389 U.S. 347, 511–12 (1967).

In his article, Professor Gershowitz observes that the *Miranda* warnings “provide virtually no protection because individuals typically waive them.”<sup>75</sup> The data he relies upon was gathered in the early 1990s. Even if his data is reliable for 2011, there are still reasons *Miranda* should apply.

Later in his article, Professor Gershowitz suggests that this tendency to waive the *Miranda* rights also extends to and encompasses passwords.<sup>76</sup> And there are a number of reported cases in which precisely this occurred,<sup>77</sup> along with a few cases in which individuals refused to provide passwords.<sup>78</sup> I am not sure we can draw any reliable inferences from the fact that there seem to be more cases in which suspects waived *Miranda* and gave up passwords than cases in which they did not. It seems reasonable to assume that those who surrender passwords to the authorities are more likely to be prosecuted than those who do not; and those who are prosecuted are more likely to crop up in reported cases than those who do not.

People will no doubt continue to waive their Fifth Amendment and/or *Miranda* rights and surrender passwords. I, though, think it is premature to assume that this is and/or will be the norm, so the use of passwords will do “little to curb” police use of search incident to examine cell phones and other digital devices.<sup>79</sup>

---

75. Gershowitz, *supra* note 1, at 1172 (citing Richard A. Leo, *Inside the Interrogation Room*, 86 J. CRIM. L. & CRIMINOLOGY 266, 276 (1996)).

76. *See* Gershowitz, *supra* note 1, at 1175.

77. *See, e.g.*, United States v. Okoro, No. 00-5050, 2000 WL 924613, at \*5 (6th Cir. June 27, 2000); United States v. Grady, No. 4:09CR00485JCH, 2010 WL 441513, at \*9 (E.D. Mo. Feb. 4, 2010); United States v. Patt, No. 06-CR-6016L, 2008 WL 2915433, at \*4 (W.D.N.Y. July 24, 2008); United States v. Jennings, CR. No. 2:06cr126-WHA, 2007 WL 1589505, at \*1 (M.D. Ala. Mar. 2, 2007); Commonwealth v. Purdy, SJC-10739, 2011 WL 1421367, at \*2 (Mass. Apr. 15, 2011).

78. *See* United States v. Diermyer, No. 3:10-cr-071-HRH-JDR, 2010 WL 4683550, at \*2 (D. Alaska Nov. 12, 2010); Griffin-El v. Beard, No. 06-2719, 2009 WL 2929802, at \*2 (E.D. Pa. Sept. 8, 2009).

79. *See* Gershowitz, *supra* note 1, at 1175.